REMARKS

The Examiner has rejected Claims 1, 4, 7, 10, 11, 14, 19, 22, 25, 28, 29, and 32 under 35 U.S.C. 103(a) as being unpatentable over Tatebayashi, Key Distribution Protocol for Digital Mobile Communication Systems, in view of Mizikovsky, U.S. Patent No.: 5,748,734. Applicant respectfully disagrees with this rejection, especially in view of the amendments made hereinabove.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*,947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991). Applicants respectfully assert that at least the first and third elements of the *prima facie* case of obviousness have not been met.

With respect to the first element of the *prima facie* case of obviousness, the Examiner states that it would have been obvious to one of ordinary skill in the art at the time the invention was made to the generate the common cryptographic key of Tatebayashi in the nodes as well as the network center in order to enhance the security of wireless communication infrastructure as taught in Mizikovsky. Applicant respectfully disagrees with this proposition, especially in view of the vast evidence to the contrary.

Just by way of example, Tatebayashi suggests the establishment of a cryptographic key at a network center. See excerpt below.

> "The network center, in response to receiving the first ciphertext signal and the second ciphertext signal, decodes these as the first key-encryption-key signal and the second key-

> encryption-key, respectively, using a public-key-decoding device. Thus the network center has the first and second key-encryption-key signals r1 and r2. The network center then can encrypt the second key-encryption-key signal r2 with the first key-encryption-key signal r1 using the classical-key-encoding device, employing any type of classical encryption device." (See Section 3 - page 3, 4th paragraph)

This teaching is in direct contrast with applicant's claimed establishment of a cryptographic key at a second node.

Thus, contrary to the Examiner's arguments, applicant's claimed feature would have been unobvious in view of Tatebayashi, since Tatebayashi *teaches away* from any sort of "establishing the cryptographic key at the second node using the first partial key value and a second partial key value created by the second node" (emphasis added), as claimed. *In re Hedges*, 783 F.2d 1038, 228 USPQ 685 (Fed. Cir. 1986).

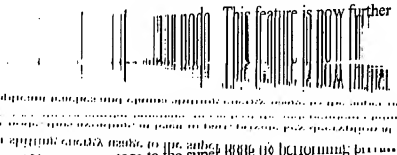
With respect to the third element of the *prima facie* case of obviousness, it is noted that the Examiner has not even attempted to make a specific prior art showing of applicant's claimed "energy usage is shifted to the super node by performing private key decryption at the super node" (see each of the independent claims). Only applicant teaches and claims such a feature for establishing a cryptographic key for use between a first node and a second node using a super node, wherein the first node and the second node are energy-limited and the super node has abundant energy.

To this end, applicant respectfully asserts that at least the first and third element of the *prima facie* case of obviousness have not been met, since the prior art reference fails to teach or suggest all the claim limitations, and it would not be unobvious to modify the prior art reference, as suggested by the Examiner. A notice of allowance or a specific prior art showing of each of the foregoing limitations, in combination with the remaining claim elements, is respectfully requested.

Despite the foregoing stark differences and in the spirit of expediting the prosecution of the present application, applicant now claims the following in each of the independent claims:

"utilizing a combination of public key cryptography and symmetric key cryptography with symmetric key encryption being used in initial exchanges between the first, second and super nodes in order to authenticate the first and second nodes to the super node, and further shifting energy usage to the super node by performing private key decryption at the super node, thus avoiding, at least in part, private key decryption at the first and second nodes" (see this or similar language in each of the independent claims).

Again, only applicant teaches and claims shifting energy usage to the super node



super node, and further shifting energy usage to the super node by performing private key decryption at the super node, thus avoiding, at least in part, private key decryption at the first and second nodes" (see this or similar language in each of the independent claims).

Again, only applicant teaches and claims shifting energy usage to the super node by performing private key decryption at the super node. This feature is now further emphasized by the claimed utilization of a combination of public key cryptography and symmetric key cryptography with symmetric key encryption being used in initial exchanges between the first, second and super nodes in order to authenticate the first and second nodes to the super node, thus avoiding, at least in part, private key decryption at the first and second nodes.

A notice of allowance or a specific prior art showing of such feature, in combination with the remaining claim elements, is respectfully requested.

It is further noted that the Examiner's rejection with respect to applicant's dependent claims is further replete with deficiencies. Specifically, with respect to Claim 4 et al., it appears that the Examiner relies on col. 7, lines 9-65 from Mizikovsky to meet applicant's claimed "sending a third message from the second node to the super node, wherein the third message includes the second partial key value encrypted using the public key belonging to the super node; recovering the second partial key value at the super node by decrypting using the private key; securely communicating the second partial key value to the first node; and establishing the cryptographic key at the first node using the first partial key value and the second partial key value."

Applicant respectfully disagrees. Mizikovsky simply fails to even suggest any sort of sending a third message from the second node to the super node, including the contents that are specifically claimed.

Again, applicant respectfully asserts that at least the first and third element of the *prima facie* case of obviousness have not been met, since the prior art reference fails to teach or suggest all the claim limitations, and it would not be obvious to modify the prior art reference, as suggested by the Examiner.

It further appears that the rejection of the remaining claims is also replete with deficiencies. Again, a notice of allowance or a specific prior art showing of each of such limitations, in combination with the remaining claim elements, is respectfully requested.

Applicant further brings the Examiner's attention to new Claim 39 which is presented for full consideration.

> "A method for establishing a cryptographic key for use between a first node and a second node using a super node, wherein the first node and the second node are energy-limited and the super node has abundant energy, the method comprising:
>
> sending a first message from the first node to the super node, the first message including a first partial key value encrypted using a public key belonging to the super node, the encrypting with the public key requiring less energy than decrypting with a private key corresponding to the public key;
>
> recovering the first partial key value at the super node by decrypting using the private key;
>
> securely communicating the first partial key value to the second node;
>
> establishing the cryptographic key at the second node using the first partial key value and a second partial key value created by the second node; and

utilizing a combination of public key cryptography and symmetric key cryptography with symmetric key encryption being used in initial exchanges between the first, second and super nodes in order to authenticate the first and second nodes to the super node, and further shifting energy usage to the super node by performing private key decryption at the super node, thus avoiding, at least in part, private key decryption at the first and second nodes;

wherein a second message is sent from the first node to the second node, wherein the second message includes a first message authentication code;

wherein the first partial key value is authenticated at the second node using the first message authentication code;

wherein the method further comprises:

sending a third message from the second node to the super node, wherein the third message includes the second partial key value encrypted using the public key belonging to the super node;

recovering the second partial key value at the super node by decrypting using the private key;

securely communicating the second partial key value to the first node; and

establishing the cryptographic key at the first node using the first partial key value and the second partial key value;

wherein a fourth message is sent from the second node to the first node, wherein the fourth message includes a second message authentication code;

wherein the second partial key value is authenticated at the first node using the second message authentication code;

wherein securely communicating the first partial key value to the second node includes:

encrypting the first partial key value at the super node using a second node symmetric key creating a first encrypted partial key value, wherein the second node symmetric key is received in the third message;

transmitting the first encrypted partial key value to the second node; and

decrypting the first encrypted partial key value at the second node to recover the first partial key value;

wherein the second node symmetric key is validated using a certificate provided by a recognized certificate authority and wherein the certificate is included in the third message;

wherein the certificate includes validation information for a plurality of symmetric keys and wherein a new second node symmetric key is selected periodically from the plurality of symmetric keys;

wherein the second node symmetric key is saved at the super node so that a subsequent key establishment can use symmetric key encryption for encrypting the first partial key value;

wherein securely communicating the second partial key value to the first node includes:

encrypting the second partial key value at the super node using a first node symmetric key creating a second encrypted partial key value, wherein the first node symmetric key is received in the first message and wherein the first node symmetric key is encrypted using the public key belonging to the super node;

transmitting the second encrypted partial key value to the first node; and

decrypting the second encrypted partial key value at the first node to recover the second partial key value;

wherein the first node symmetric key is validated using a certificate provided by a recognized certificate authority and wherein the certificate is included in the first message;

wherein the certificate includes validation information for a plurality of symmetric keys and wherein a new first node symmetric key is selected periodically from the plurality of symmetric keys;

wherein the first node symmetric key is saved at the super node so that a subsequent key establishment can use symmetric key encryption for encrypting the second partial key value;

wherein establishing the cryptographic key at the first node involves creating a hash of the first partial key value and the second partial key value;

wherein establishing the cryptographic key at the second node involves creating a hash of the first partial key value and the second partial key value;

wherein trust of the super node is established at the first node by validating a certificate provided by a recognized certificate authority and presented to the first node by the super node;

wherein trust of the super node is established at the second node by validating a certificate provided by a recognized certificate authority and presented to the second node by the super node" (see Claim 39).

Yet again, a notice of allowance or a specific prior art showing of each of the foregoing limitations, in combination with the remaining claim elements, is respectfully requested.

To this end, all of the pending independent claims are deemed allowable, along with any dependent claims dependent therefrom.

Reconsideration is respectfully requested.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. Applicants are enclosing a check to pay for the added claims. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P255).

Respectfully submitted,
Zilka-Kotab, PC

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100